Edição 20 | 2022

cybernews.

Tozzini Freire.
ADVOGADOS

sumário

///// Realidade Brasileira

ANPD avança na regulamentação da aplicação de sanções

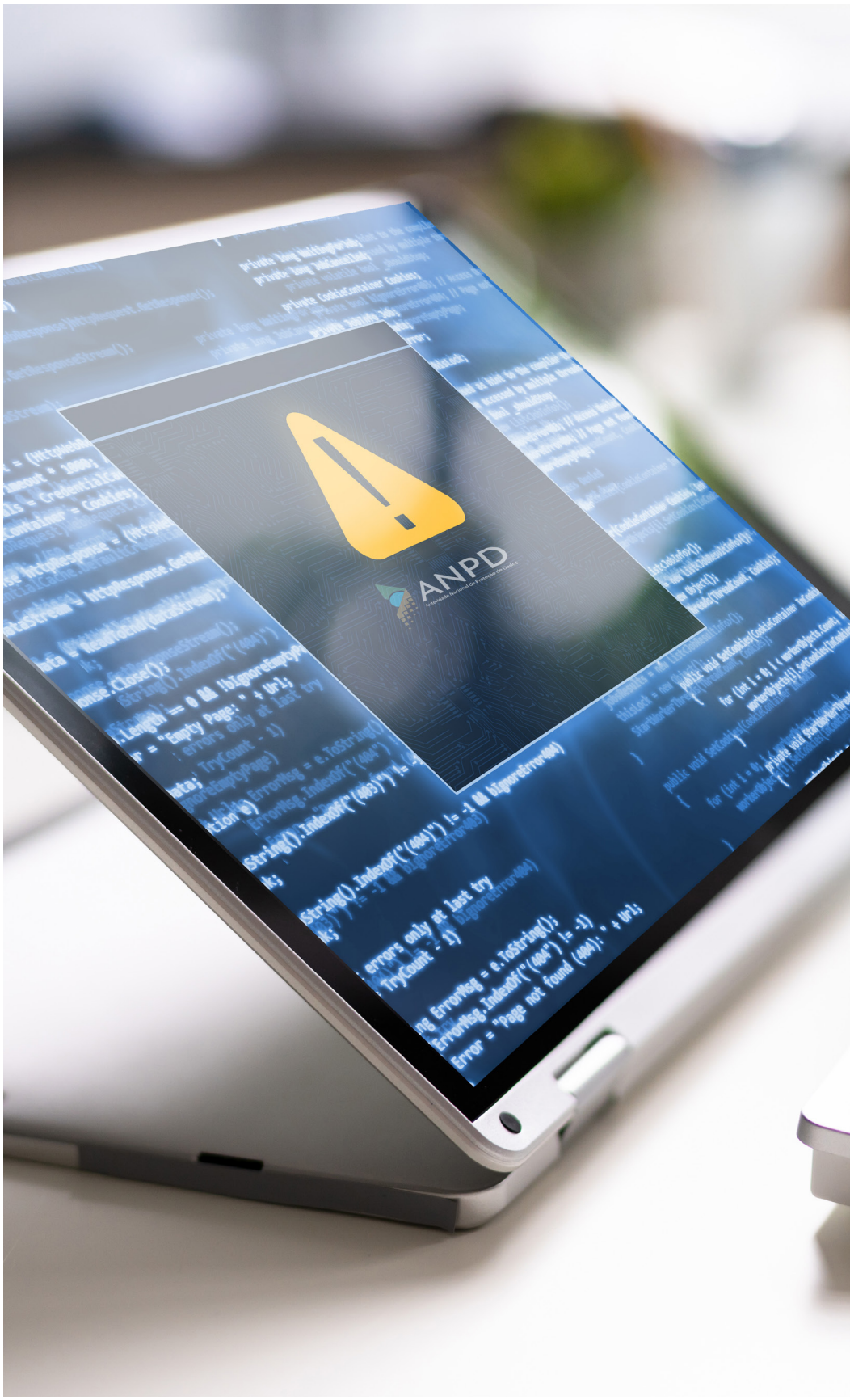
A Autoridade Nacional de Proteção de Dados (ANPD) abriu nova consulta pública sobre minuta de Resolução que regulamenta a aplicação de sanções pela ANPD, dispostas nos arts. 52 e 53 da Lei Geral de Proteção de Dados (LGPD).

A norma proposta busca complementar o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 1/2021, ao estabelecer regras claras, em especial os parâmetros e critérios, para a aplicação de sanções administrativas, i.e., a dosimetria das sanções.

As contribuições devem ser realizadas por meio da plataforma Participa Mais Brasil e puderam ser enviadas até 15 de setembro 2022.

Além disso, a ANPD também já disponibilizou o Relatório de Análise de Impacto Regulatório, no qual são detalhados os parâmetros e critérios para aplicação de sanções e cálculo do valor-base das multas, bem como os votos proferidos pelos diretores da Autoridade (acesse aqui).

Essas iniciativas estão alinhadas com a agenda regulatória da ANPD, que previa o início da regulamentação das normas de fiscalização e aplicação de sanção ainda em 2022.



Recomendação 34/2022 sobre boas práticas a serem adotadas para mitigar riscos inerentes à segurança cibernética

Em 08 de setembro de 2022, o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) em conjunto com a Secretaria do Governo Digital (SGD) e o Serviço Federal de Processamento de Dados (SERPRO) emitiram a Recomendação 34/2022 sobre boas práticas a serem adotadas a fim de mitigar os principais riscos inerentes à segurança cibernética.

Em razão da pandemia de COVID-19, o trabalho remoto foi intensificado e, consequentemente, a preocupação com a segurança cibernética também, o que justifica a relevância de atentar a essas medidas preventivas.

Quanto às políticas, recomenda-se estabelecer planos de gestão de backup com armazenamento seguro dos dados, de atualização de sistemas computacionais, de segurança de acesso remoto quando a organização utilizar VPN e duplo/múltiplo fator de autenticação, e de política de monitoramento de dispositivos corporativos.

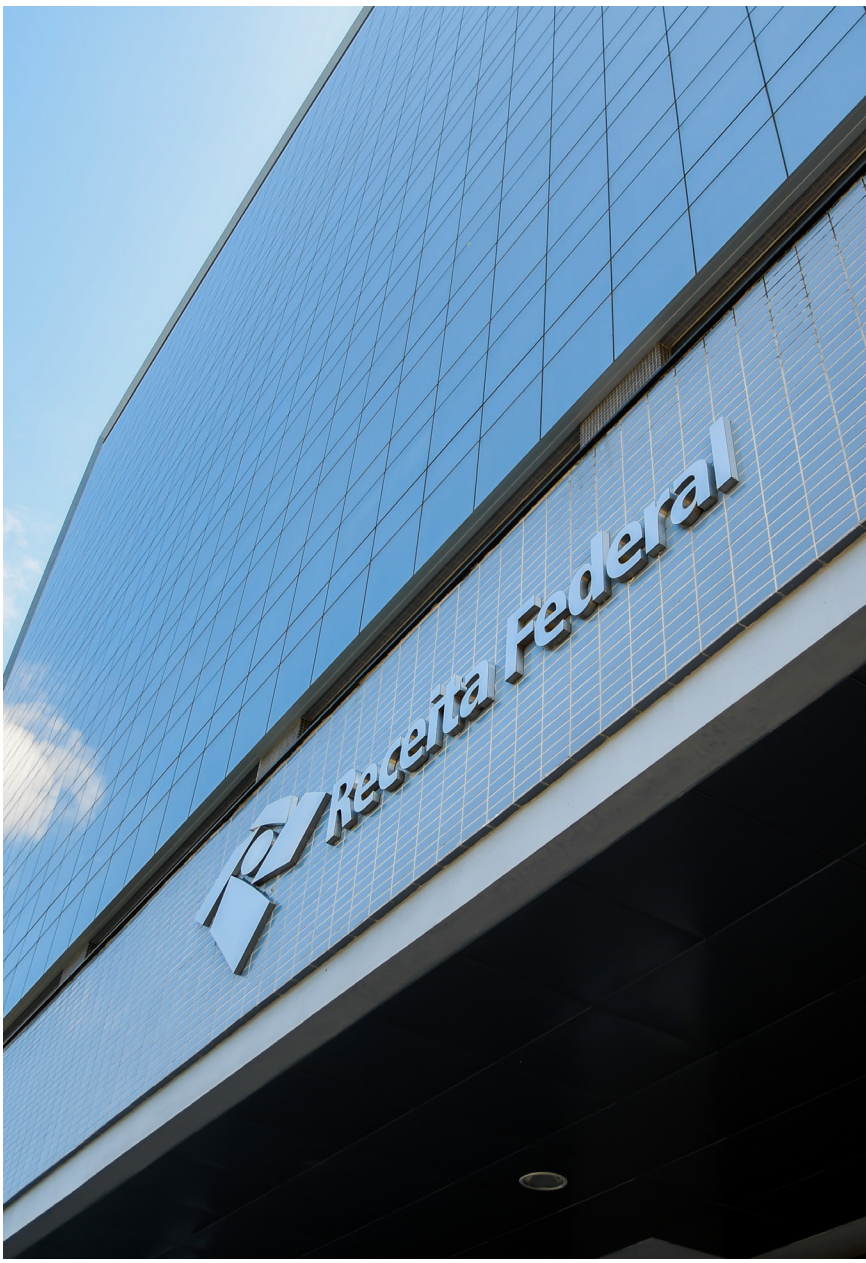
Além dessas medidas, também foram ações recomendadas pelas autoridades: realizar testes periódicos de recuperação de dados, revisar constantemente planos estratégicos de segurança e políticas de segurança cibernética e da informação, utilizar senhas fortes e manter registro centralizado de eventos de sistemas (*logs*) e em ambiente controlado.

ANPD divulga Nota Técnica que conclui a análise sobre o tratamento de dados entre Receita Federal e SERPRO

No dia 05 de agosto de 2022, a ANPD divulgou para o público a Nota Técnica nº 68/2022/CGF/ANPD, a qual versa sobre a análise realizada pela ANPD após a publicação da Portaria RFB nº 167/2022, de abril deste ano, que autoriza o Serviço Federal de Processamento de Dados (SERPRO) a disponibilizar acesso, para terceiros, de dados e informações da Receita.

A Nota, em suma, divulga o encerramento do procedimento de fiscalização, de modo a concluir que não há incompatibilidade no tratamento de dados operado pela Portaria RFB nº 167/2022 com o previsto pela legislação de proteção de dados pessoais. Nesse sentido, a ANPD compreendeu, através dos Relatórios de Impacto apresentados pela Receita Federal, que a referida Portaria objetiva fornecer os instrumentos necessários para o acesso a dados que já eram, em sua maioria, dados públicos por força de normativos e de políticas públicas, como informações sobre CPF, CNPJ e certidão negativa de débitos.

Portanto, não se verificou a incompatibilidade com a LGPD do tratamento dos dados trazidos pela Portaria RFB nº 167/2022, haja vista que se trata de dados pessoais que estão inseridos em políticas públicas e que possuem finalidade definida.



ANPD inicia tomada de subsídios sobre tratamento de dados pessoais de alto risco

A ANPD iniciou, em 29 de agosto de 2022, a nova tomada de subsídios sobre o tratamento de dados pessoais de alto risco, que ficará aberta para contribuições até 29 de setembro de 2022 por meio da plataforma Participa Mais Brasil (acesse aqui).

Essa tomada de subsídios é baseada no artigo 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, datada de 27 de janeiro de 2022, que estabelece os critérios para definição do tratamento de alto risco ao titular de dados.

O artigo 4º dispõe que o tratamento de dados pessoais será considerado de alto risco quando atender a pelo menos um critério geral e um critério específico, cumulativamente. Dentre eles, os critérios gerais são tratamento de dados pessoais (a) em larga escala, ou (b) que possa afetar significativamente interesses e direitos fundamentais dos titulares.

Já os critérios específicos podem ser o tratamento com (a) uso de tecnologias emergentes ou inovadoras, (b) vigilância ou controle de zonas acessíveis ao público, (c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, ou (d) utilização de dados pessoais sensíveis ou de dados pessoais de grupos vulneráveis, como crianças, adolescentes e idosos.

ANPD abre nova tomada de subsídios sobre tratamento de dados pessoais de crianças e adolescentes

A ANPD abriu, em 08 de setembro de 2022, a nova tomada de subsídios acerca do tratamento de dados pessoais de crianças e adolescentes, que ficará aberta para contribuições até 07 de outubro de 2022 por meio da plataforma Participa Mais Brasil (acesse aqui).

Conforme divulgado pela ANPD, essa tomada de subsídios almeja analisar quais hipóteses legais seriam aplicáveis ao tratamento dos dados de crianças e adolescentes. Apesar de a LGPD prever seção específica para o tratamento de dados de crianças e de adolescentes, ainda há controvérsias acerca da correta interpretação de determinados dispositivos da lei por profissionais da área.

Nesse sentido, em razão da insegurança jurídica advinda pela indefinição de quais hipóteses legais autorizam o tratamento de dados pessoais de crianças e adolescentes, a ANPD estruturou um estudo preliminar sobre o tema, a fim de fomentar o debate público e subsidiar futura tomada de decisão pela ANPD.

Dessa forma, haja vista as divergências constatadas e a importância do tema, a ANPD iniciou a Tomada de Subsídios para receber contribuições da sociedade, com o intuito de coletar posicionamentos de pessoas interessadas no assunto, para que as múltiplas perspectivas sejam levadas em consideração na regulamentação do tema.

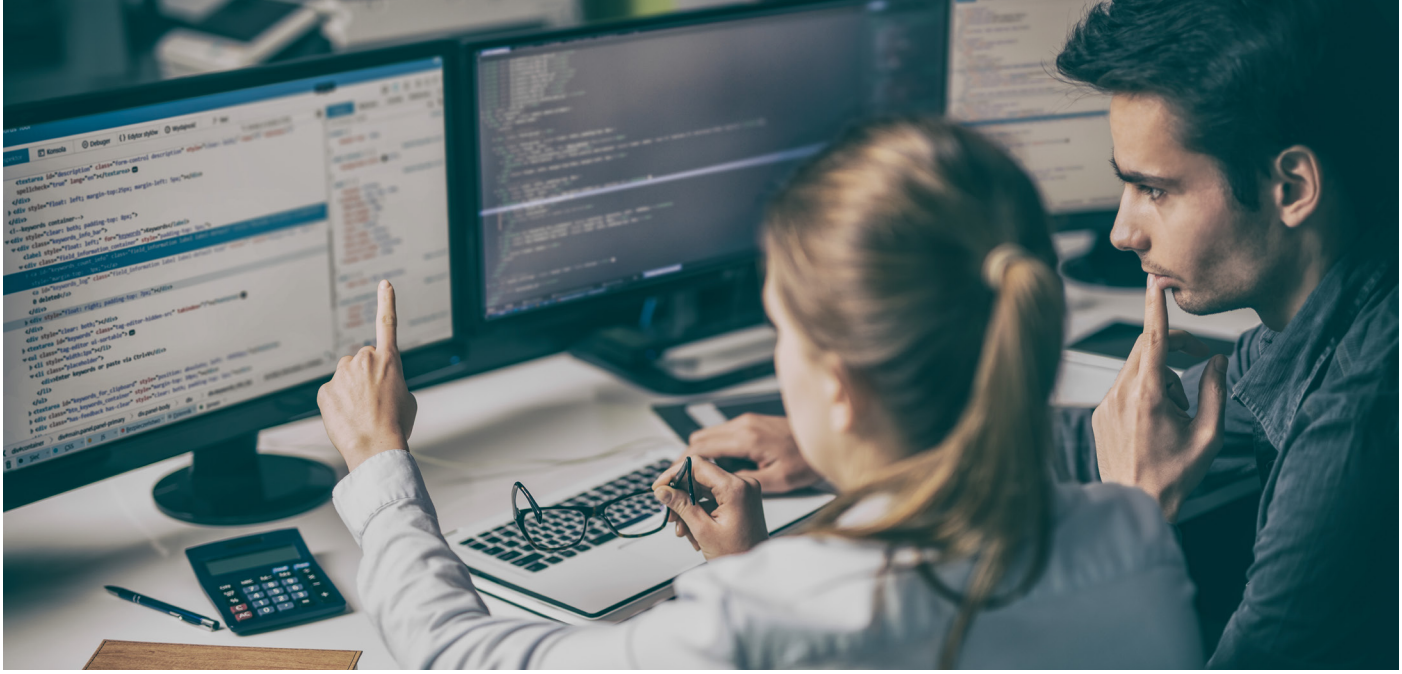
Guia 3/2022 sobre “Dark patterns” em interfaces de plataformas de mídia social: como reconhecê-los e evitá-los

Em primeiro lugar, vale dizer que o termo “dark patterns”, ou “padrões escuros”, foi criado em 2010 pelo cientista britânico Harry Brignull, para se referir a estratégias de design utilizadas para promover comportamentos contrários às leis de proteção de dados pessoais e de direito do consumidor. Nesse sentido, utilizam-se determinadas estratégias para manipular o comportamento dos usuários.

À vista dos impactos que os dark patterns podem ter para a proteção de dados pessoais, o European Data Protection Board (EDPB) emitiu o Guia nº 3/2022 em março de 2022. Nos termos da definição apresentada pelo Guia, dark patterns podem ser entendidos como “interfaces e experiências de usuário implementadas em plataformas de mídia social que levam os usuários a tomar decisões não intencionais, relutantes e potencialmente prejudiciais sobre o tratamento de seus dados pessoais”.

Nessa perspectiva, o Guia objetiva apresentar recomendações para que web designers e internautas do meio cibernético possam analisar e evitar a implementação de formas de dark patterns que possam infringir as leis de proteção de dados pessoais.

Além disso, foram enumerados seis tipos de dark patterns, quais sejam: (i) “Overloading”, entendido pela exposição dos usuários a um alto volume de informações e solicitações, com o intuito de induzi-los a compartilhar mais dados ou, involuntariamente, permitir o tratamento de dados pessoais contra seus interesses; (ii) “Skipping”, o qual revela-se na estruturação da interface de tal modo que os indivíduos relevem a importância da proteção de seus dados; (iii) “Stirring”, compreendido pela manipulação das escolhas que o indivíduo faria apelando para suas emoções ou usando “nudges” (“cutucadas”) visuais; (iv) “Hindering”, entendido como a imposição de barreiras digitais aos consumidores, de forma a dificultar ou tornar impossível a conclusão do processo de gerenciamento dos dados coletados e tratados por determinada companhia; (v) “Fickle”, que consiste na projeção de uma interface instável e inconsistente, de maneira a dificultar que os usuários naveguem nos diversos mecanismos de controle de proteção de dados e compreendam a finalidade do tratamento; (vi) “Left in the dark”, sendo o design de uma interface de modo a ocultar informações ou ferramentas de controle de proteção de dados, ou deixar os usuários inseguros sobre como seus dados são tratados e que tipo de controle eles podem ter sobre eles para resguardar seus direitos.



Autoridade de Proteção de Dados de Guernsey publica guia sobre as obrigações de privacidade de empresas a funcionários

A Autoridade de Proteção de Dados de Guernsey, na última semana de agosto, divulgou nos seus canais oficiais um guia que trata das obrigações dos empregadores no tratamento de dados pessoais, bem como dos princípios aplicáveis ao contexto da relação de trabalho.

A publicação vem em um cenário de aumento da complexidade nas relações de trabalho, com o tratamento cada vez maior de dados pessoais. De acordo com o guia, é importante dar atenção para os dados pessoais sensíveis coletados no contexto da relação de emprego, como a origem étnica e a orientação sexual do empregado, uma vez que tais dados demandam um maior nível de segurança.

Além disso, o guia reitera a importância de se orientar por princípios de tratamento de dados pessoais como, por exemplo, a adequação e a finalidade do tratamento, a necessidade da coleta de tais dados pessoais, assim como a confidencialidade daqueles dados pessoais perante terceiros.

ICO publica guia para pequenas empresas responderem a solicitações de proteção de dados

Em agosto de 2022, a Information Commissioner's Office (ICO) – a autoridade independente do Reino Unido responsável pela manutenção do interesse público nas questões envolvendo dados pessoais – publicou um guia para orientar pequenas empresas a como proceder quando receberem uma solicitação relativa à proteção de dados pessoais.

Às vezes empregados, clientes, contratados ou outros titulares de dados podem não estar satisfeitos com a forma com a qual empresa tratou seus dados pessoais, então o guia serve para orientar quanto às medidas adequadas a serem tomadas nessas situações, que ajudarão a manter a reputação da empresa que se preocupa com a proteção de dados pessoais.

O guia determina seis etapas para tanto: acusar o recebimento da solicitação, entender o problema específico relacionado à solicitação, fornecer regularmente atualizações ao titular dos dados, registrar as medidas e ações adotadas em resposta à solicitação, responder formalmente o indivíduo com o resultado da investigação ou solução do problema e, por fim, revisar as lições aprendidas com a solicitação recebida para evitar solicitações futuras.

Além de detalhar as medidas a serem tomadas em cada etapa, a ICO também recomenda que na comunicação com o titular dos dados sempre seja utilizada uma linguagem clara, específica e direta, para evitar possíveis mal-entendidos.

Ao seguir todas essas etapas para responder a uma solicitação de titular de dados, você se mostrará preocupado em resolver o problema, o que ajuda a construir maior confiança dos clientes, empregados, contratados e outros titulares de dados.

Estrangeiros agora têm direito de acessar dados pessoais tratados por instituições canadenses

A partir de 13 de julho de 2022, estrangeiros não residentes no Canadá, pelo Privacy Act, terão direito a acessar os dados pessoais que estejam sendo tratados por instituições do governo federal. A extensão do direito foi dada pela Ordem de Extensão nº 3 à Lei de Proteção de Dados Canadense.

Até então, os estrangeiros fora do Canadá eram dependentes de um serviço oferecido por um terceiro que agiria como mandatário e faria o pedido de acesso em nome do estrangeiro titular de dados pessoais. Agora, o pedido pode ser feito pelo próprio titular.

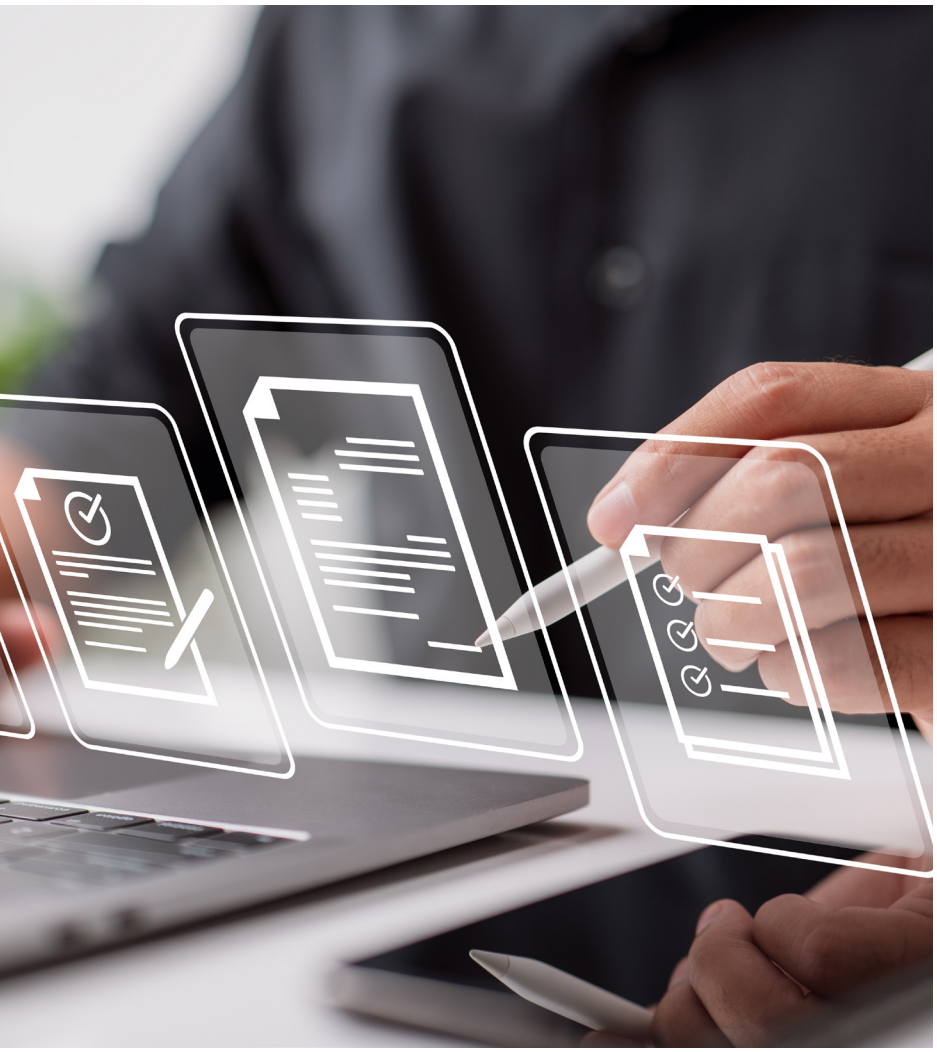
Além disso, a Ordem de Extensão também garantiu aos estrangeiros a possibilidade de submeter reclamações à Autoridade de Proteção de Dados canadense, caso entendam que seu acesso aos dados pessoais esteja sendo negado, atrasado ou que as informações estejam imprecisas.

Autoridades de Supervisão dos Estados Bálticos lançam uma inspeção coordenada da conformidade do tratamento de dados pessoais no aluguel de veículos de curta duração

Em setembro de 2021, durante reunião das Autoridades Supervisoras (AS) de proteção de dados pessoais dos Estados Bálticos, concluiu-se que uma cooperação mais estreita entre as autoridades supervisoras contribuirá para uma fiscalização mais eficiente do tratamento de dados pessoais nos Estados Bálticos. À vista disso, as AS dos Estados Bálticos instituíram uma inspeção preventiva coordenada acerca da conformidade do tratamento de dados pessoais no mercado de aluguel de veículos automotores por curtos períodos de tempo.

Tal iniciativa surgiu com o objetivo de desenvolver recomendações para melhorar a proteção dos dados pessoais nesse segmento de mercado, abordando de forma proativa as potenciais ameaças aos dados pessoais dos cidadãos. Nesse sentido, as AS acordaram que a fiscalização será exercida sobre as empresas que oferecem o aluguel de veículos de curta duração, cujos principais clientes são pessoas físicas.

Dessa forma, todas as empresas do setor que ofereçam os seus serviços nos Estados Bálticos serão monitoradas. No que diz respeito à sua independência decisória, cada AS pode expandir o âmbito da fiscalização às empresas que também exerçam atividades em um único Estado-Membro do báltico.



TJSP entende que é necessária prova do dano para responsabilização civil

A 35ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo negou provimento a um recurso de apelação após entender que a consumidora não havia provado a ocorrência de dano moral indenizável decorrente do vazamento de seus dados pessoais por empresa concessionária de energia elétrica. O relator afirmou, ainda, que os dados vazados não eram sensíveis e não comprometiam a dignidade da autora.

A consumidora havia acionado a Justiça em busca de uma indenização por danos morais, alegando que o vazamento de seus dados pessoais a levou a experimentar inúmeros dissabores, tal qual o recebimento de mensagens indesejadas e propagandas pelo celular. O juízo de primeiro grau julgou improcedente a demanda, decisão esta que foi mantida pelo tribunal com o julgamento do recurso de apelação. Segundo o Tribunal, "afastada a ocorrência de abalo moral, a improcedência da demanda é medida de rigor".

O entendimento final firmado pelo Tribunal foi o de que, não obstante a responsabilidade objetiva da concessionária quanto ao tratamento de dados (art. 42 da LGPD), a responsabilização civil força a análise da existência de dano, o que não foi comprovado pela consumidora.

TSE decide que dados relativos aos candidatos deverão ser mantidos públicos

O plenário do Tribunal Superior Eleitoral decidiu que manterá públicos os dados relativos aos candidatos das eleições 2022. Mantendo ocultos apenas dados como endereço, e-mail e telefones pessoais, o colegiado também entendeu que a declaração de bens deve ser feita de forma pública.

A discussão sobre o tema se iniciou após pedido feito por Luciano Reginaldo Fulcro, eleito suplente de vereador pelo município de Guarulhos. O Tribunal aceitou a solicitação para que seus dados fossem excluídos da plataforma em razão de ameaças que sofreu durante as eleições.

O ministro Alexandre de Moraes, no entanto, em sessão ocorrida no mês de agosto, votou a favor da publicação de dados relativos aos candidatos, argumentando que a LGPD é lei geral, enquanto a Legislação Eleitoral é lei específica, não se sujeitando às restrições da lei geral.

O ministro Edson Fachin, relator do caso, já havia votado anteriormente pela manutenção da transparência como regra, limitando-a apenas para dados que dizem respeito à intimidade e privacidade dos candidatos. Defendeu, assim, a manutenção da plataforma como forma de controle social, que possibilita que a sociedade possa fiscalizar as candidaturas de seus representantes.

STF decide pela necessária observância da LGPD no compartilhamento de dados pela administração pública

No começo deste mês, o Supremo Tribunal Federal deu início ao julgamento da constitucionalidade do Decreto nº 10.046/2019, que regula o compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão, bem como o Comitê Central de Governança de Dados.

O Decreto é objeto de duas ações no STF (ADI 6.649 e ADPF 695) que, em julgamento ocorrido no dia 15/09/2022, foram julgadas parcialmente procedentes para dar ao Decreto interpretação conforme o previsto na Constituição Federal. Os ministros do STF entenderam que o Decreto não resguarda os direitos dos cidadãos por permitir uma difusão de dados sensíveis entre os entes governamentais, fugindo do que a LGPD prevê.

Conforme voto do ministro Gilmar Mendes, relator das ações, o compartilhamento de dados por parte do poder público deve ser limitado ao mínimo necessário, condicionado somente a determinados interesses públicos que se comprovem legais, necessários e legítimos, além da necessidade de que haja uma rigorosa fiscalização e controle das atividades realizadas pelos órgãos públicos, em estrita observância à LGPD. Ainda, firmou o entendimento de que, se as diretrizes da LGPD forem desobedecidas, o Estado responderá objetivamente pelos danos causados às pessoas.

Além disso, conforme voto do relator, foi determinada a reformulação em 60 dias do Comitê Geral de Governança de Dados, pois, composto apenas por órgãos do poder executivo, deve passar a contar também com a participação da sociedade civil. Este foi, entretanto, ponto de divergência no voto dos ministros André Mendonça e Kassio Nunes Marques, que entenderam que esta reorganização deve apenas ocorrer a partir do dia 31 de dezembro deste ano.

O ministro Fachin também apresentou voto divergente, possuindo o posicionamento de que todo o decreto é inconstitucional, mas concordando com as diretrizes de interpretação fixadas pelo relator. Já os ministros Alexandre de Moraes, Roberto Barroso, Luiz Fux, Dias Toffoli, Cármen Lúcia, Ricardo Lewandowski e Rosa Weber acompanharam Gilmar Mendes em seus votos.

STF discute violação à LGPD por exposição de processo criminal ou trabalhista em sistemas de pesquisa

O Tribunal de Justiça do Estado do Rio Grande do Sul julgou improcedente uma demanda sobre dados pessoais, entendendo que é lícita a exposição de processos públicos por meio da busca por dados pessoais dos envolvidos na internet. A parte Ré recorreu ao Supremo Tribunal Federal, para que a decisão tomada seja firmada em âmbito nacional.

De acordo com o procurador-geral da República, Augusto Aras, o recurso não deve ser provido, pois a divulgação irrestrita de informações de ações trabalhistas e criminais no meio virtual, a partir de pesquisa com dados pessoais, violaria a LGPD: "O tratamento de dados pessoais de acesso público por parte dos agentes de tratamento, de forma a permitir a publicização ampla e a consulta pelo nome das partes de informações de processos trabalhistas e criminais exorbita a autorização de tratamento de dados pela LGPD, tendo em conta a inexistência de justificação baseada em finalidade legítima e específica em concreto e a violação aos direitos do titular".

Segundo Aras, a consulta pública de ações trabalhistas e criminais somente é permitida, no sistema dos tribunais, a partir do número do processo, não devendo ser possível identificar o caso com dados pessoais dos envolvidos.

Ele alega, ainda, que essas amplas informações divulgadas podem causar danos aos envolvidos, os quais terão sua imagem vinculada a processos trabalhistas e criminais, violando também o direito à privacidade, intimidade e proteção de dados. Por fim, entende que aqueles que divulgam irregularmente dados pessoais deverão indenizar a vítima em caso de eventuais danos. O caso ainda pende de julgamento pelo Supremo Tribunal Federal e está sendo tratado no âmbito do sistema de repercussão geral, sob o Tema 1141 (ARE 1307386).

Secretarias do Estado de Pernambuco foram intimadas pelo MPPE a se adequarem à LGPD

Foi constatada, pelo Ministério Público de Pernambuco, a possibilidade de que o direito à proteção de dados pessoais tenha sido violado por parte da Secretaria Estadual de Desenvolvimento Social, Criança e Juventude. Assim, o órgão ministerial recomendou que as Secretarias Estaduais realizem adequações para que a LGPD possa ser cumprida, ressaltando que as "operações de tratamento de dados pessoais por parte de entidades públicas ou privadas devem ser pautadas nos fundamentos na LGPD, como o respeito à privacidade, a autodeterminação informativa, os direitos humanos, a dignidade e o exercício da cidadania pelas pessoas, dentre outros".

Conforme recomendação publicada no Diário Oficial Eletrônico do MPPE, em 05/09/2022, as Secretarias Estaduais têm prazo de dez dias para se manifestar sobre o acatamento ou não da recomendação.

Ex-diretor hospitalar é condenado por acessar ilegalmente registros de pacientes

No início de agosto, Christopher O'Brien, ex-diretor da fundação hospitalar inglesa South Warwickshire NHS Foundation Trust, foi condenado por acessar, sem justificativa razoável e sem autorização da fundação, os dados pessoais de 14 pacientes.

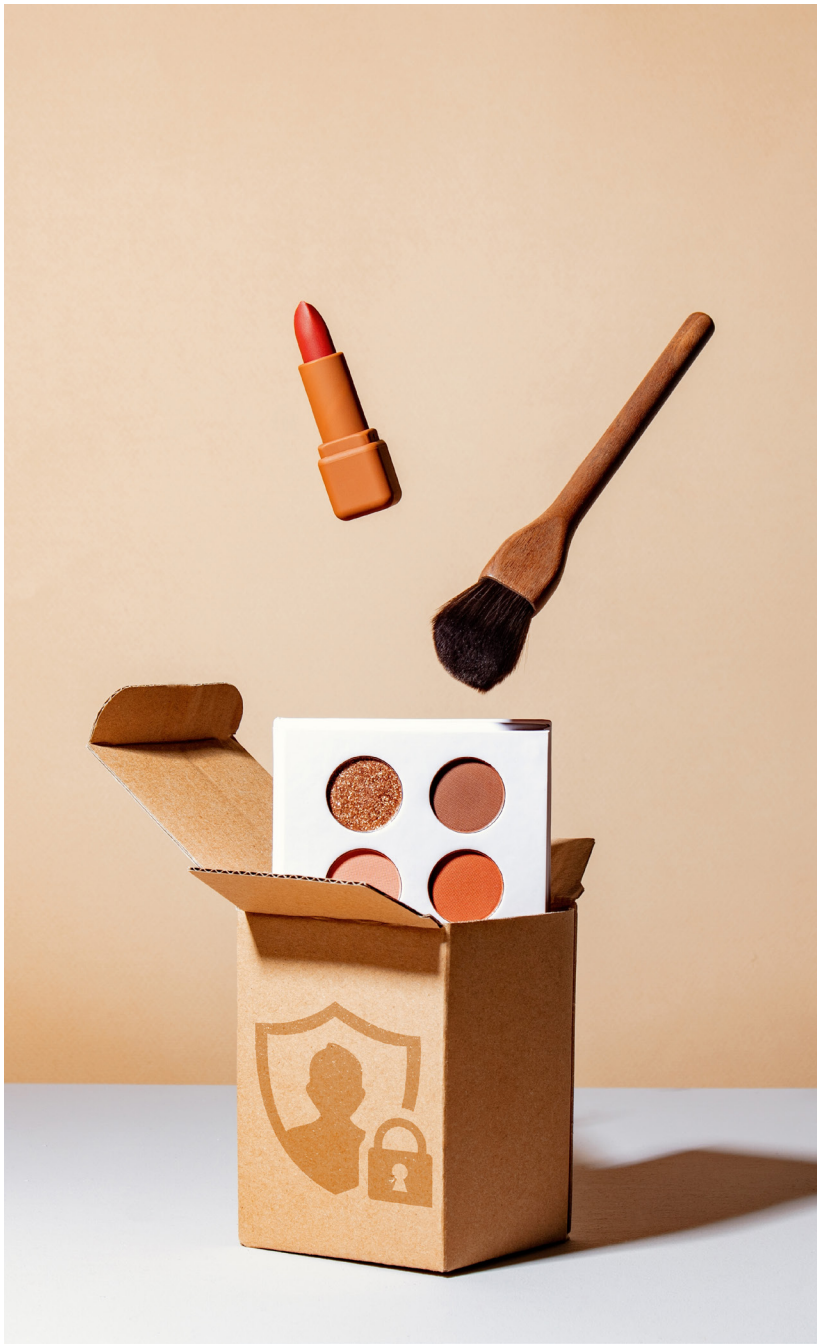
A Corte de Magistrados de Coventry, responsável por julgar o caso do ex-administrador, condenou-o ao pagamento de compensação a 12 dos pacientes, totalizando cerca de £3,000 (três mil libras). O'Brien declarou-se culpado das acusações.

Pacientes do hospital de Warwick, Inglaterra, que eram inclusive conhecidos de O'Brien, disseram que o vazamento dos dados pessoais os intimidou a voltarem às consultas médicas, causando uma situação de profunda preocupação e ansiedade.

A Autoridade de Proteção de Dados Britânica, a ICO, por meio do Diretor de Investigações Stephen Eckersley, insistiu que organizações reafirmem as responsabilidades relacionadas a proteção de dados e governança da informação, em especial ao lidar com dados pessoais sensíveis.

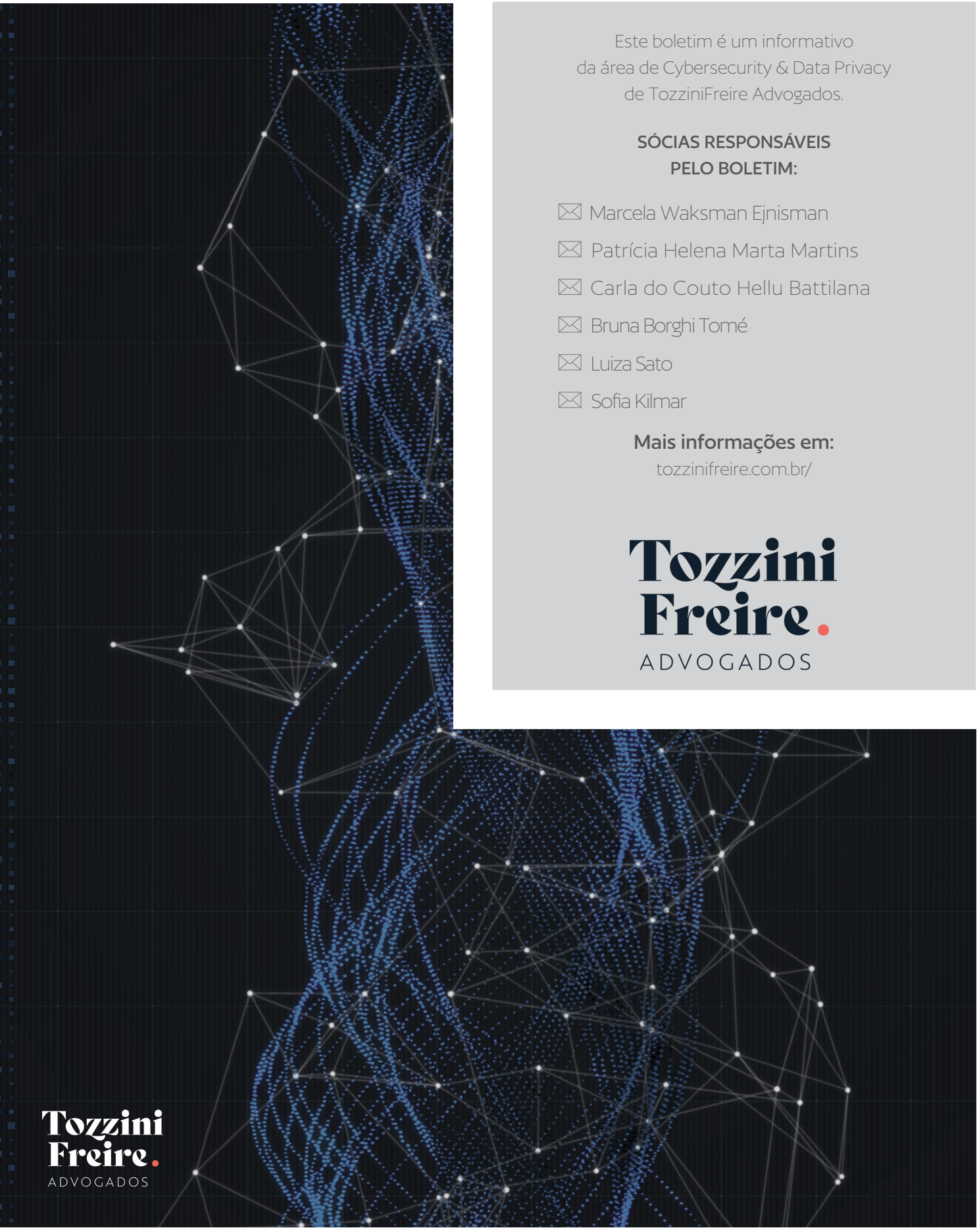
Sephora é a primeira empresa a ser multada por violação da Lei de Privacidade do Consumidor da Califórnia

Em agosto de 2022, o procurador-geral da Califórnia, Rob Bonta, anunciou um acordo da promotoria com a empresa francesa de cosméticos Sephora Inc., que foi a primeira empresa a ser multada pela Lei de Privacidade do Consumidor da Califórnia (CCPA) – a lei "Não Venda", que dispõe sobre os direitos dos consumidores de saber como as empresas tratam seus dados e optar por não permitir sua venda – e deverá pagar uma multa de 1,2 milhão de dólares e cumprir uma série de obrigações de conformidade com a lei.



De acordo com informações obtidas do procurador-geral, a violação da lei pela Sephora resultou da não divulgação aos consumidores de que estava vendendo seus dados pessoais e não conseguiu processar solicitações de usuários para desativar a venda desses dados por meio de controles de privacidade, violando assim a CCPA. No mais, a empresa francesa não corrigiu ou tentou mitigar essas violações dentro do período de 30 dias atualmente permitido pela CCPA.

Entre as obrigações que a Sephora deverá cumprir estão: alterar sua política de privacidade online para esclarecer que vende dados pessoais, disponibilizar meios para que os consumidores optem por não vender seus dados, adaptar seus contratos de provedor de serviços para estarem em conformidade com a CCPA, e fornecer relatórios ao escritório do procurador-geral da Califórnia relacionados à venda de dados pessoais, o status de seus relacionamentos com provedores de serviços e seus esforços para honrar a especificação Global Privacy Control (GPC).



Imagens: Shutterstock

Este boletim é um informativo
da área de Cybersecurity & Data Privacy
de TozziniFreire Advogados.

SÓCIAS RESPONSÁVEIS PELO BOLETIM:

✉ Marcela Waksman Ejnisman
✉ Patrícia Helena Marta Martins
✉ Carla do Couto Hellu Battilana
✉ Bruna Borghi Tomé
✉ Luiza Sato
✉ Sofia Kilmar

Mais informações em:
tozzinifreire.com.br/

Tozzini
Freire.
ADVOGADOS